AFFIDAVIT IN SUPPORT OF SUPPLEMENTAL SEARCH WARRANT

I, Collin Scott, being duly sworn, hereby depose and state that the following is true to the best of my information, knowledge, and belief:

INTRODUCTION AND AGENT BACKROUND

1. I have been employed as a Special Agent of the FBI since January 2018, and am currently assigned to the Salt Lake City Field Office and FBI Child Exploitation Task Force. Prior to my employment with the FBI, I obtained a Bachelor's degree in Information Technology, and was employed with a computer software company for five years. As a result of my training and experience, I am familiar with information technology and its use in criminal activities. Since joining the FBI, I have investigated violations of federal law, and am currently investigating federal violations concerning child pornography and the sexual exploitation of children.

2. As a federal agent, I am authorized to investigate violations of laws of the United States and am a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

PURPOSE OF THE AFFIDAVIT

3. This Affidavit is submitted in support of an application for a search warrant for the following place, also described in **Attachment A** (the "Subject Property"):

> The contents of the Microsoft Online Services ID stephen.c.shunn@gmail.com and associated Microsoft OneDrive account, located at Microsoft Online Services, 1 Microsoft Way, Redmond, Washington 98052-6399.

for the items described in **Attachment B**, which are evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252A(a)(2) (Receipt and Distribution of Child Pornography) and (a)(5)(B) (Possession of or Access with Intent to View Child Pornography) (the "Subject Offenses").

4. Because this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause for the requested warrant.

5. The information contained in this Affidavit is based on my training and experience, as well as information imparted to me by other law enforcement officers involved in this investigation.

STATUTORY AUTHORITY

6. This investigation concerns alleged violations of 18 U.S.C. §§ 2252, and 2252A, relating to material involving the sexual exploitation of minors, as described more fully below:

a. 18 U.S.C. § 2252(a)(1) prohibits knowingly transporting or shipping in interstate or foreign commerce, by computer or mail, any visual depiction of minors engaging in sexually explicit conduct.

b. 18 U.S.C. § 2252(a)(2) prohibits knowingly receiving or distributing, by computer or mail, any visual depiction of minors engaging in sexually explicit conduct that has been mailed, shipped, or transported in interstate or foreign commerce. That section also prohibits knowingly reproducing any visual depiction of minors engaging in sexually explicit conduct for distribution in interstate or foreign commerce by any means, including by computer or the mail.

c. 18 U.S.C. § 2252(a)(4) prohibits possessing one or more books, magazines, periodicals, films, or other materials which contain visual depictions of minors engaged in sexually explicit conduct that have been transported in interstate or foreign commerce, or that were produced using materials that had traveled in interstate or foreign commerce.

d. 18 U.S.C. § 2252A(a)(1) prohibits knowingly mailing, transporting, or shipping child pornography in interstate or foreign commerce by any means, including by computer.

e. 18 U.S.C. § 2252A(a)(2) prohibits knowingly receiving or distributing any child pornography that has been mailed or shipped or transported in interstate or foreign commerce by any means, including by computer.

f. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing any book, magazine, periodical, film, videotape, computer disk, or other material that contains an image of child pornography that has been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer.

DEFINITIONS

7. The following definitions apply to this Affidavit and **Attachment B** to this Affidavit:

8. "Child Pornography" includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

9. "Visual depictions" includes prints, copies of visual images, developed and undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

10. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

11. "IP Address" means Internet Protocol address, which is a unique numeric address used by computers on the Internet. Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

12. "Internet" means a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

13. In this Affidavit, the terms "computers" or "digital storage media" or "digital storage devices" may be used interchangeably, and are intended to include any physical object upon which computer data can be recorded as well as all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices capable of performing logical, arithmetic, or storage functions, including desktop and laptop computers, mobile phones, tablets, server computers, game consoles, network hardware, hard disk drives, RAM, floppy disks, flash memory, CDs, DVDs, and other magnetic or optical storage media.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

14. Computers and computer technology have revolutionized the way in which individuals interested in child pornography interact with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce

the images. There were definable costs involved with the production of pornographic images. To distribute these on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings and telephone calls.

15. The development of computers has changed this. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

16. Child pornographers can now transfer photographs from a camera onto a computer-readable format with a device known as a scanner. With the advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world.

17. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

18. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

19. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Google, Yahoo!, and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

20. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Additionally, a forensic examiner often can recover evidence suggesting whether a computer contains peer to peer software (P2P) (which is described in more detail in the following paragraphs), when the computer was sharing files, and some of the files which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

21. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all

computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

SEARCH METHODOLOGY TO BE EMPLOYED

22. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. Examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. Surveying various file directories and the individual files they contain;

d. Opening files in order to determine their contents;

e. Scanning storage areas;

f. Performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in **Attachment A**; and/or

g. Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in **Attachment B**.

PREFERENTIAL SEXUAL OFFENDERS AND THE INTERNET

23. Based upon my experience and discussions with other law enforcement officers, I have learned that there are many types of preferential sex offenders. Some of these offenders have a primary sexual interest in children and are often referred to as pedophiles. This Affidavit deals with these types of offenders. Preferential sex offenders receive sexual gratification from actual contact with children and/or from fantasy involving children, through the use of photographs and/or digital images that can be stored on computer hard drives and other types of digital recordable media (floppy diskettes, writable compact discs, writable DVDs, etc.). I am aware that these types of sex offenders often collect sexually explicit material consisting of photographs, video tapes, books, slides, and digital images, which they use for their own sexual gratification and fantasy and to show children in an attempt to lower the child's inhibitions.

24. I have learned that the Internet has provided preferential sex offenders with a virtually anonymous venue in which they can meet other people with the same or similar sexual interests. Preferential sex offenders also use the computer to electronically exchange pictures of children or of adults engaged in sexual activity with children. These images are readily and easily available on the Internet. These images can then be downloaded and stored on the computer or other forms of digital recordable media such as CD's, DVDs, USB thumb drives, floppy disks, etc., and then viewed on the computer monitor at any time. Preferential sex

offenders will also participate in chat rooms in order to communicate with other like-minded individuals and to meet children. This communication serves to legitimize their conduct and beliefs. I am also aware from training and experience that preferential sex offenders who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage to their collections of child pornography. I also know that these individuals typically maintain their child pornography collections in the privacy and security of their homes, or other secure location.

MICROSOFT ONLINE SERVICES

25. I have learned that Microsoft (aka Microsoft Live services) provides a variety of on-line services, including electronic mail ("email") access referred to as Microsoft Outlook and cloud storage referred to as OneDrive (formerly Skydrive) to the general public. Subscribers obtain an account by registering with Microsoft. During the registration process, Microsoft asks subscribers to provide basic personal information. Therefore, the computers of Microsoft are likely to contain stored electronic communications (including retrieved and un-retrieved e-mail for Microsoft subscribers) and information concerning subscribers and their use of Microsoft services, such as account access information, e-mail transaction information, and account application information.

26. In general, an e-mail that is sent to a Microsoft subscriber is stored in the subscriber's "mail box" on Microsoft's servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Microsoft's servers indefinitely.

27. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to Microsoft's servers, and then transmitted to its end destination. Microsoft often saves a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the Live.com server, the e-mail can remain on the system indefinitely.

28. A Microsoft subscriber can also store files, including e-mails, address books, contacts, pictures, and other files, on servers maintained and/or owned by Microsoft.

29. Subscribers to Microsoft might not store on their home computers copies of the e-mails stored in their Microsoft account. This is particularly true when they access their Microsoft account through the web, or if they do not wish to maintain particular e-mails or files in their residence.

30. In general, e-mail providers like Microsoft ask each of their subscribers to provide certain personal identifying information when registering for an e-mail account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers such as alternative e-mail addresses.

31. Additionally, a Microsoft subscriber can create a Microsoft account with any valid email address even if the email account is not a Microsoft domain. As a result, an individual with an AOL or Gmail email address can create a Microsoft account with their Gmail or AOL email address and be able to access Microsoft's services, to include Microsoft's cloud storage service (OneDrive) or email service (Outlook.com). As a result, a Gmail or AOL user can register for a Microsoft account, have access to a OneDrive account, and then configure their Outlook account so that the user's Gmail or AOL emails, contact lists, and address books can be stored in their Outlook account on Microsoft's servers.

MICROSOFT ONEDRIVE

32. **Microsoft OneDrive** (previously SkyDrive, Windows Live SkyDrive and Windows Live Folders) is a file hosting service that allows users to upload and sync files to a cloud storage and then access them from a Web browser or their local device. It is part of the suite of online services formerly known as Windows Live and allows users to keep the files private, share them with contacts, or make the files public. Publicly shared files do not require a Microsoft account to access. Users of Microsoft OneDrive's online storage have the ability to make the files stored in their account private, shared with others whom they provide access, or shared to the public. As a result, an offender can store a significant amount of child pornography online and not have to store the contraband on a computer. Additionally, the offender can provide access to these files to other offenders.

33. In general, e-mail providers like Microsoft ask each of their subscribers to provide certain personal identifying information when registering for an e-mail account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers such as alternative e-mail addresses.

34. E-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular

logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

35. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the warrant to require Microsoft to disclose to the government copies of the records and other information (including the content of communications) particularly described in **Attachment B**.

BACKGROUND OF INVESTIGATION

36. Based on my knowledge and experience, and on information received from other individuals, including law enforcement officers, as well as their reports, as set forth below, I have learned the following.

37. On September 11, 2024, a federal search warrant was issued by Magistrate Judge Paul D. Kohler in Case No. 2:24-mj-904-PK authorizing law enforcement to search 574 South Willow Crossing, Lehi, Utah, including the residential building, outbuildings, and appurtenances thereto (collectively, the "South Willow property") for evidence of violations of the Subject Offenses, including all devices found on the South Willow property. Additionally, the warrant authorized law enforcement to search and seize any devices found on the person of Stephen Craig Shunn.

38. On September 12, 2024, the search warrant was executed at the South Willow property. During the search, devices belonging to Stephen Craig Shunn were seized and thereafter processed and forensically analyzed at the FBI Intermountain West Regional

Computer Forensics Laboratory. Contemporaneous with the execution of the warrant at the South Willow property, law enforcement appeared at Mr. Shunn's place of employment and, pursuant to the warrant, searched his person, which yielded a Samsung Galaxy A54 Model: SM-A546U cellphone (the "Samsung phone").

39. Upon review of the results of the forensic examination of the Samsung phone, I confirmed that the application Microsoft OneDrive was installed on the phone and was associated with the email account Stephen.c.shunn@gmail.com.

40. I also viewed over 30 cached images associated with the OneDrive account that depicted child pornography. At least ten of the images depicted prepubescent female children being orally and vaginally raped by adult males.

41. On November 13, 2024, a federal grand jury sitting in the District of Utah returned a two-count Indictment against Stephen Craig Shunn charging him with violations of 18 U.S.C. §§ 2252A(a)(2) (Receipt of Child Pornography) and (a)(5)(B) (Possession of or Access with Intent to View Child Pornography) based on evidence arising out of the investigation summarized in this Affidavit.

42. Based on the aforementioned information, I respectfully submit there is probable cause to believe that an individual using the email account Stephen.c.shunn@gmail.com that is associated with a Microsoft OneDrive account contains violations of the Subject Offenses. Further, I submit there is probable cause to believe that evidence pertaining to the Subject Offenses are stored in the OneDrive account, as more fully described in **Attachment A**. Rule 41 of the Federal Rules of Criminal Procedure authorizes the government to seize and retain

evidence and instrumentalities of a crime for a reasonable time, and to examine, analyze, and test them.

43. Based upon my knowledge, training and experience, and consultations with FBI experts, I know that searching and seizing information from computers often requires agents to seize most or all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following:

a. The volume of evidence. Computer storage devices (like hard disks, diskettes, tapes, laser disks, Bernoulli drives, thumb drives, removable storage devices, etc.) can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence of instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site.

b. Technical requirements. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources and from destructive codes imbedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

44. In order to ensure that forensic examiners search only those computer accounts and/or files necessary to find evidence of violations of 18 U.S.C. §§ 2252 and 2252A, this Affidavit and application for a search warrant seeks authorization to permit employees of the Intermountain West Regional Computer Forensics Laboratory to assist agents in the execution of this warrant.

CONCLUSION

45. Based on the investigation described above, I respectfully submit there is probable cause to believe that evidence pertaining to the receipt, distribution, and possession of child pornography is currently stored, concealed, and located in the OneDrive account associated with the email account Stephen.c.shunn@gmail.com, as more fully described in **Attachment A**, including evidence, fruits and instrumentalities of violations of 18 U.S.C. §§ 2252 and 2252A described in **Attachment B**.

/s/ Collin Scott

COLLIN SCOTT, Special Agent
Federal Bureau of Investigation

SUBSCRIBED and SWORN before me this 27th day of November, 2024.

The Honorable Dustin B. Pead
United States Chief Magistrate Judge

Approved:

TRINA A. HIGGINS
United States Attorney

/s/ Mark Y. Hirata

MARK Y. HIRATA
Assistant United States Attorney

ATTACHMENT A
PROPERTY TO BE SEARCHED

The contents of the Microsoft Online Services ID stephen.c.shunn@gmail.com and associated Microsoft OneDrive account, located at Microsoft Online Services, 1 Microsoft Way, Redmond, Washington 98052-6399.

ATTACHMENT B

ITEMS TO BE SEIZED

The following items to be seized constitute fruits, instrumentalities and evidence of violations of 18 U.S.C. §§ 2252A(a)(2) (Receipt and Distribution of Child Pornography) and (a)(5)(B) (Possession of or Access with Intent to View Child Pornography) (the "Subject Offenses"):

1. Images or visual depictions of child pornography.

2. Records and information containing child erotica, including texts, images and visual depictions of child erotica.

3. Any and all information, notes, software, documents, records, or correspondence, in any format and medium, pertaining to violations of the Subject Offenses.

4. Any and all information, notes, documents, records, or correspondence, in any format or medium, concerning communications about child pornography or sexual activity with or sexual interest in minors.

5. Any and all information, notes, documents, records, or correspondence, in any format or medium, concerning Internet activity reflecting a sexual interest in minors or child pornography.

6. Any and all information, notes, software, documents, records, or correspondence, in any form and medium pertaining to any minor who is, or appears to be, the subject of any visual depiction of child pornography, child erotica, sexual activity with other minors or adults, or of sexual interest, or that may be helpful in identifying any such minors.

7. Any and all address books, names, and lists of names and addresses of individuals who may have been contacted by use of the computer or by other means for the purpose of committing violations of the Subject Offenses.

8. Any and all information, notes, documents, records, or correspondence, in any format or medium, concerning membership in online groups, clubs, or services that provide or make accessible child pornography.

9. Any and all information, records, documents, invoices and materials, in any format or medium, that concern any accounts with an Internet Service Provider pertaining to violations of the Subject Offenses.

10. Any and all information, records, documents, invoices and materials, in any format or medium, that concern e-mail accounts, online storage, or other remote computer storage pertaining to violations of the Subject Offenses.

11. Any and all information, documents, records, photos, videos, or correspondence, in any format or medium, pertaining to occupancy or ownership of the account, or that aid in the identification of persons involved in violations of the Subject Offenses.

12. Credit cards, credit card information, bills and payment records pertaining to violations of the Subject Offenses.

13. Information about usernames or any online accounts or email addresses that include Comcast or other Internet Service Providers used in the commission of violations of the Subject Offenses.

DEFINITIONS:

14. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

15. "Child Pornography" is defined in 18 U.S.C. § 2256(8), which includes as any visual depiction of sexually explicit conduct involving the use of a minor; a digital image, computer image, or computer-generated image that is, or is indistinguishable from that of a minor engaged in sexually explicit conduct; or a visual depiction that has been created, adapted, or modified to appear than an identifiable minor is engaging in sexually explicit conduct.

16. "Visual depiction" includes prints, copies of visual images, developed and undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

17. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions; this also includes texts or discussions regarding minors engaged in sexual acts or conduct.

18. As used above, the terms "computers" or "digital storage media" or "digital storage devices" may be used interchangeably, and are intended to include any physical object upon which computer data can be recorded as well as all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices capable of performing logical, arithmetic, or storage functions, including desktop and laptop computers, mobile phones, tablets, server computers, game consoles, network hardware, hard disk drives, RAM, floppy disks, flash memory, CDs, DVDs, and other magnetic or optical storage media.